IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 11bf D4.0 CR for sensing replay counter | | | | |
| Date: 2024-08-20 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Po-Kai Huang | Intel |  |  | po-kai.huang@intel.com |
| Ido Ouzieli |  |  |  |
| Cheng Chen |  |  |  |
| Nehru Bhandaru | Broadcom |  |  | nehru.bhandaru@broadcom.com |

Abstract

This submission proposes resolutions for the following CIDs:

6016, 6017, 6186

Revisions:

* Rev 0: Initial version of the document.

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGbf D4.0 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbf D4.0 Draft. (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents). TGbf Editor: Editing instructions preceded by “TGbf Editor” are instructions to the TGbf editor to modify existing material in the TGbf draft. As a result of adopting the changes, the TGbf editor will execute the instructions rather than copy them to the TGbf Draft.***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 6016 | 12.5.4.4.4 | 205.21 | Since there is no indication in the GCMP header that a frame is a sensing frame vs. another type of action frame, the receiver cannot determine the correct replay counter before decryption and hence cannot perform replay detection before decryption. | Provide a mechanism in the GCMP header to identify the correct replay counter, in a manner that is extensible/usable by other future procedures. | Revised –  We add solution similar to 11az and use joint bit indication to efficiently use the bit in the security header.  TGbf editor to make the changes shown in 11-24/1422r0 under all headings that include CID 6016 |
| 6017 | 12.5.2.4.4 | 204.46 | Since there is no indication in the CCMP header that a frame is a sensing frame vs. another type of action frame, the receiver cannot determine the correct replay counter before decryption and hence cannot perform replay detection before decryption (as explicitly allowed in the baseline 12.5.2.4.4, step (I)). | Provide a mechanism in the CCMP header to identify the correct replay counter, in a manner that is extensible/usable by other future procedures. | Revised –  We add solution similar to 11az and use joint bit indication to efficiently use the bit in the security header.  TGbf editor to make the changes shown in 11-24/1422r0 under all headings that include CID 6016 |
| 6186 | 12.5.2.4.4 | 204.46 | The cited text indicates that the receiver needs to maintain a separate replay counter for sensing frames. Currently in the standard prior to P802.11bf, any type of frame that uses a separate reply counter is signalled in either the header or the CCMP header. Same issue for GCMP on p205.21 | Add signaling in either the 802.11 header or the CCMP/GCMP header to signal a protected sensing frame. | Revised –  We add solution similar to 11az and use joint bit indication to efficiently use the bit in the security header.  TGbf editor to make the changes shown in 11-24/1422r0 under all headings that include CID 6016 |

**Discussion:**

The suggestion to have bits in security header to indicate specific replay counter of Protected Sensing frames for early discard is similar to the suggestion in 11az to have bits in security header to indicate specific replay counter of Protected Fine Timing frames for early discard.

11az solution does not require AAD change. Instead, post decryption validation is used. Specially, if the bit is altered by the attacker:

* FTM bit is set to 1 but change to 0
  + If receiver early discard the frame, then this is fine because an altered frame needs to be discarded
  + If receiver does not early discard the frame using normal replay counter, then the receiver will decrypt the frame, realize that it is FTM and discard the frame.
* FTM bit is set to 0 but change to 1
  + If receiver early discard the frame, then this is fine because an altered frame needs to be discarded
  + If receiver does not early discard the frame using FTM replay counter, then the receiver will decrypt the frame, realize that it is not FTM and discard the frame.

In sum, post decryption validation will capture the inconsistency and discard the frame. See quote texts below.

*See 12.5.2.2 (CCMP MPDU format) for a description of how the PN is encoded in the CCMP header. The following processing rules are used to detect replay:*

1. *If the receiver performs replay detection prior to decryption, then the receiver shall check that the replay counter used to detect replays is correct and discard the frame if incorrect. In particular, the separate replay counter for individually addressed Protected Fine Timing frames shall be used if the FTM subfield of the CCMP of GCMP header (Figure 12-15 (Expanded CCMP MPDU) or Figure 12-28 (Expanded GCMP MPDU)) signals that the MPDU is a Protected Fine Timing frame; it shall not be used otherwise.*

(Note that revme somehow pushes both CCMP and GCMP design under CCMP clause, which is a bug.)

We propose to follow similar principle of 11az to provide the bits in security header for indication of sensing frmae before decryption and use similar post decryption validation rules. We directly add two more bits to allow enough number of entries to be used later.

To mitigate the concern that we use one bit for one replay counter, we use bit Bit 2, Bit 3 and Bit 4 (called reply counter index) jointly to indicate FTM (001) and Sensing frames (010), where other entries will be reserved and 000 means Not FTM and Not Sensing.

|  |  |  |  |
| --- | --- | --- | --- |
| B2 of Key ID octet | B3 of Key ID octet | B4 of Key ID octet | Indication in a protected individually addressed Action frame |
| 0 | 0 | 0 | Not FTM and Not Sensing |
| 0 | 0 | 1 | FTM |
| 0 | 1 | 0 | Sensing |
| 0 | 1 | 1 | Reserved |
| 1 | 0 | 0 | Reserved |
| 1 | 0 | 1 | Reserved |
| 1 | 1 | 0 | Reserved |
| 1 | 1 | 1 | Reserved |

There are no backward compatibility issues because these three bits are only used for individually addressed action frames. For legacy STA that supports FTM and does not support Sensing frame, the STA will never see Bit 2 or Bit 3 to 1 from honest peer and any frame with Bit 2 or Bti 3 set to 1 from peer will just be in wrong setting.

**Proposal: (#6016)**

*TGbf editor: Modify Clause 12.5.2.2 as follows (track change on):*

### 12.5.2.2 CCMP MPDU format

Change the text and Figure 12-15 as shown:

Figure 12-15 (Expanded CCMP MPDU) depicts the MPDU when using CCMP.

**B0 B1 B2 B4 B5 B6 B7**

**MAC Header**

**CCMP Header**

8 octets

**Data (PDU)**

≥ 1 octet

**FCS**

4 octets

**MIC**

variable

**PN0**

**PN1**

**Rsvd**

**Rsvd**

**Ext**

**IV**

**Key**

**ID**

**PN2**

**PN3**

**PN4**

**PN5**

Key ID octet

Encrypted

**Replay Counter**

**Index**

Figure 12-15—Expanded CCMP MPDU

(…existing texts….)

Bits 2–4 of the Key ID octet are for the Replay Counter Index subfield in a protected individually addressed Action frame that is a Protected Fine Timing frame or a Protected Sensing frame (see Table 9-81 (Category values) and Table XXX). In other protected individually addressed frames, bits 2–4 are reserved, i.e., set to 0.

Table XXX – Indication of Replay Counter Index subfield

|  |  |  |  |
| --- | --- | --- | --- |
| B2 of Key ID octet | B3 of Key ID octet | B4 of Key ID octet | Indication in a protected individually addressed Action frame |
| 0 | 0 | 0 | Not FTM and Not Sensing |
| 0 | 0 | 1 | FTM |
| 0 | 1 | 0 | Sensing |
| 0 | 1 | 1 | Reserved |
| 1 | 0 | 0 | Reserved |
| 1 | 0 | 1 | Reserved |
| 1 | 1 | 0 | Reserved |
| 1 | 1 | 1 | Reserved |

The ExtIV subfield (bit 5) of the Key ID octet (#3056)is always set to 1 for CCMP.(#1386)

Bits 6–7 of the Key ID octet are for the Key ID subfield. The remaining bits of the Key ID octet are reserved.(#1386)

(…existing texts….)

**12.5.2.4.4 PN and replay detection**

See 12.5.2.2 (CCMP MPDU format) for a description of how the PN is encoded in the CCMP header. The following processing rules are used to detect replay:

1. If the receiver performs replay detection prior to decryption, then the receiver shall check that the replay counter used to detect replays is correct and discard the frame if incorrect. In particular, the separate replay counter for individually addressed Protected Fine Timing frames shall be used if the Replay Counter Index subfield of the CCMP (Figure 12-15 (Expanded CCMP MPDU) signals that the MPDU is a Protected Fine Timing frame; the separate replay counter for individually addressed Protected Fine Timing frames shall not be used otherwise. The separate replay counter for individually addressed Protected Sensing frames shall be used if the Replay Counter Index subfield of the CCMP header (Figure 12-15 (Expanded CCMP MPDU)) signals that the MPDU is a Protected Sensing frame; the separate replay counter for individually addressed Protected Sensing frames shall not be used otherwise.

*TGbf editor: Modify Clause 12.5.2.2 as follows (track change on):*

### 12.5.4.2 GCMP MPDU format

Change the text and Figure 12-28 as shown:

Figure 12-28 (Expanded GCMP MPDU) shows the MPDU format when using GCMP.

**B0 B1 B2 B4 B5 B6 B7**

**MAC Header**

**GCMP Header**

8 octets

**Data (PDU)**

≥ 1 octet

**FCS**

4 octets

**MIC**

variable

**PN0**

**PN1**

**Rsvd**

**Rsvd**

**Replay Counter Index**

**Ext**

**IV**

**Key**

**ID**

**PN2**

**PN3**

**PN4**

**PN5**

Key ID octet

Encrypted

Figure 12-28—Expanded GCMP MPDU

(…existing texts….)

Bits 2–4 of the Key ID octet are for the Replay Counter Index subfield in a protected individually addressed Action frame that is a Protected Fine Timing frame or a Protected Sensing frame (see Table 9-81 (Category values) and Table XXX). In other protected individually addressed frames, bits 2–4 are reserved, i.e., set to 0.

Table XXX – Indication of Replay Counter Index subfield

|  |  |  |  |
| --- | --- | --- | --- |
| B2 of Key ID octet | B3 of Key ID octet | B4 of Key ID octet | Indication in a protected individually addressed Action frame |
| 0 | 0 | 0 | Not FTM and Not Sensing |
| 0 | 0 | 1 | FTM |
| 0 | 1 | 0 | Sensing |
| 0 | 1 | 1 | Reserved |
| 1 | 0 | 0 | Reserved |
| 1 | 0 | 1 | Reserved |
| 1 | 1 | 0 | Reserved |
| 1 | 1 | 1 | Reserved |

The ExtIV subfield (bit 5) of the Key ID octet is always set to 1 for GCMP.

The third octet of the GCMP Header field is reserved.(#1385)

Bits 6–7 of the Key ID octet are for the Key ID subfield. The remaining bits of the Key ID octet are reserved.

(…existing texts….)

**12.5.4.4.4 PN and replay detection**

To effect replay detection, the receiver extracts the PN from the GCMP header. See 12.5.4.2 (GCMP MPDU format) for a description of how the PN is encoded in the GCMP header. The following processing rules are used to detect replay:

1. If the receiver performs replay detection prior to decryption, then the receiver shall check that the replay counter used to detect replays is correct and discard the frame if incorrect. In particular, the separate replay counter for individually addressed Protected Fine Timing frames shall be used if the Replay Counter Index subfield of the GCMP header (Figure 12-28 (Expanded GCMP MPDU)) signals that the MPDU is a Protected Fine Timing frame; the separate replay counter for individually addressed Protected Fine Timing frames shall not be used otherwise. The separate replay counter for individually addressed Protected Sensing frames shall be used if the Replay Counter Index subfield of the GCMP header (Figure 12-28 (Expanded GCMP MPDU)) signals that the MPDU is a Protected Sensing frame; the separate replay counter for individually addressed Protected Sensing frames shall not be used otherwise.